
Subject: [stehor4 51589398] DreamHost Security Alert – Site Compromised

From: DreamHost Security Bot (secalerts@dreamhost.com)

To: shornik@yahoo.com;

Date: Wednesday, November 16, 2011 9:01 PM

Hello,

During a recent security scan on our servers it has come to our attention one of your DreamHost hosted websites have been compromised. It would appear that an unknown malicious party has modified your site's .htaccess file in order to redirect traffic destined for your website to their own site (or you have become generous and chose to re-route your site's traffic to a "sweepstakes and contests info" website.)

We have taken steps to remove this redirect by removing the affected lines in your site's .htaccess file, and renamed the original infected .htaccess file to .htaccess.infected. Here are the locations where we found malicious .htaccess files.

/home/shornik/mydebitcredit.com.old/.htaccess
/home/shornik/robinshermano.com/.htaccess
/home/shornik/mydebitcredit.com/.htaccess

During the scan we identified the following suspected backdoors (the method the attackers used to edit your site's .htaccess file above)

/home/shornik/mydebitcredit.com/wp-blog-header.php
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files/learn_sandy.php
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files/olav_steady.php
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files/wp1.5_2.0/wp-admin/ibinc.php
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files/wp1.5_2.0/wp-search.php
/home/shornik/mydebitcredit.com/wp-content/themes/wpglass/catalog.php
/home/shornik/mydebitcredit.com/CaptchaSecurityImages.php
/home/shornik/mydebitcredit.com/wp-config-sample.php
/home/shornik/mydebitcredit.com/install.php
/home/shornik/mydebitcredit.com/wp-mail.php
/home/shornik/mydebitcredit.com/send_simpleform.php
/home/shornik/mydebitcredit.com/wp-rss2.php
/home/shornik/mydebitcredit.com/wp-activate.php
/home/shornik/mydebitcredit.com/wp-login.php
/home/shornik/mydebitcredit.com/wp-rdf.php
/home/shornik/mydebitcredit.com/wp-comments-post.php
/home/shornik/mydebitcredit.com/wp-load.php
/home/shornik/mydebitcredit.com/wp-config.php
/home/shornik/mydebitcredit.com/xmlrpc.php
/home/shornik/mydebitcredit.com/wp-feed.php
/home/shornik/mydebitcredit.com/wp-pass.php
/home/shornik/mydebitcredit.com/index.php

/home/shornik/mydebitcredit.com/mySql_Connect.php
/home/shornik/mydebitcredit.com/wp-cron.php
/home/shornik/mydebitcredit.com/wp-signup.php
/home/shornik/mydebitcredit.com/hello.php
/home/shornik/mydebitcredit.com/wp-commentsrss2.php
/home/shornik/mydebitcredit.com/wp-app.php
/home/shornik/mydebitcredit.com/wp-trackback.php
/home/shornik/mydebitcredit.com/processor.php
/home/shornik/mydebitcredit.com/wp-settings.php
/home/shornik/mydebitcredit.com/wp-register.php
/home/shornik/mydebitcredit.com/wp-atom.php
/home/shornik/mydebitcredit.com/wp-links-opml.php
/home/shornik/mydebitcredit.com/CaptchaSecurityImagest.php
/home/shornik/mydebitcredit.com/wp-rss.php

We have also done a scan on your site files and found the following directories have insecure permissions. Where we were able to, we have changed the permissions to a more secure 755 -- This change makes it so only the owner of the directory may add files in these locations.

/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/optional_files/podpress_trac
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/images
/home/shornik/mydebitcredit.com/wp-content/plugins/podpress/getid3

The existence of these pages on your website(s) is likely a sign you have been compromised, and we empathize with your problem, getting a site hacked really is no fun (but we hope this notification helps prevent this matter from being any worse.) Investigating similar attacks we have found that this specific type of compromise is connected with sites that have insecure permission on folders and may be running insecure 3rd party software (including plugins and/or themes) under your account. I would highly recommend that you:

- Update any 3rd party software under the account, including content management systems, gallery software, weblogging tools, etc. Be sure to use current, secure versions and keep them up-to-date.
- Update any plugins and/or themes on your sites (Recent attacks against websites have targeted vulnerable software such as timthumb.php which is included in wordpress themes, separate from the core files)
- Check your website(s) files for any signs of tampering (file timestamps show recent editing) or files you did not upload yourself and remove them. Looking at the reported files above should give you a good starting point.
- Check your website(s) files for any 777 directories, (e.g.. a directory that allows anyone on the server to write or edit the files in the directory; these permissions will look like rwxrwxrwx via the command line)
- Change your FTP password(s). Be sure they are at least 8 characters in length and do not contain English words. Random numbers and letters work best.

If you have any questions, please feel free to reply to this email or contact our support staff and we will be more than happy to assist you with securing your sites.

Sincerely,
The DreamHost security team